

Guía docente

200256 - CRIPTOG - Criptografía

Última modificación: 26/05/2026

Unidad responsable: Facultad de Matemáticas y Estadística
Unidad que imparte: 749 - MAT - Departamento de Matemáticas.

Titulación: GRADO EN MATEMÁTICAS (Plan 2009). (Asignatura optativa).

Curso: 2026 **Créditos ECTS:** 6.0 **Idiomas:** Catalán, Inglés

PROFESORADO

Profesorado responsable: ROBERTO GUALDI

Otros: Primer quadrimestre:
ROBERTO GUALDI - A
JORDI GUARDIA RUBIES - A

COMPETENCIAS DE LA TITULACIÓN A LAS QUE CONTRIBUYE LA ASIGNATURA

Específicas:

GM-CE2. CE-2. Resolver problemas de Matemáticas, mediante habilidades de cálculo básico y otros, planificando su resolución en función de las herramientas de que se disponga y de las restricciones de tiempo y recursos.

GM-CE4. CE-4. Desarrollar programas que resuelvan problemas matemáticos utilizando para cada caso el entorno computacional adecuado.

GM-CE6. Capacitar para resolver problemas de ámbito académico, técnico, financiero o social mediante métodos matemáticos.

Genéricas:

GM-CB5. Haber desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios multidisciplinarios posteriores con un alto grado de autonomía en disciplinas científicas en las que las Matemáticas tienen un papel significativo.

GM-CG1. CG-1. Comprender y utilizar el lenguaje matemático.

GM-CB4. CB-4. Poder transmitir información, ideas, problemas y soluciones del ámbito matemático y científico-tecnológico a un público tanto especializado como no especializado.

GM-CG2. CG-2. Conocer demostraciones rigurosas de algunos teoremas clásicos en distintas áreas de la Matemática.

GM-CG3. CG-3. Asimilar la definición de un nuevo objeto matemático, en términos de otros ya conocidos, y ser capaz de utilizar este objeto en diferentes contextos.

GM-CG4. CG-4. Saber trasladar al lenguaje matemático problemas de otros ámbitos y utilizar esta traslación para resolverlos.

GM-CG6. CG-6. Detectar deficiencias en el propio conocimiento y superarlas mediante la reflexión crítica y la elección de la mejor actuación para ampliar este conocimiento.

Transversales:

04 COE. COMUNICACIÓN EFICAZ ORAL Y ESCRITA: Comunicarse de forma oral y escrita con otras personas sobre los resultados del aprendizaje, de la elaboración del pensamiento y de la toma de decisiones; participar en debates sobre temas de la propia especialidad.

07 AAT. APRENDIZAJE AUTÓNOMO: Detectar deficiencias en el propio conocimiento y superarlas mediante la reflexión crítica y la elección de la mejor actuación para ampliar este conocimiento.

METODOLOGÍAS DOCENTES

OBJETIVOS DE APRENDIZAJE DE LA ASIGNATURA

Distinguir entre criptografía de clave privada y criptografía de clave pública.
Evaluar cuándo un criptosistema es robusto.
Comprender cómo dos partes pueden establecer un secreto compartido sobre un canal inseguro.
Conocer dos de los sistemas criptográficos de clave pública más comunes que se utilizan actualmente en aplicaciones: RSA y ECC (criptografía de curvas elípticas).
Describir algunos algoritmos de prueba de primalidad y factorización, y comprender su papel en la criptografía moderna.
Trabajar con algunas nociones básicas de curvas elípticas sobre campos finitos.
Comprender el uso de los retículos en la criptografía postcuántica.

HORAS TOTALES DE DEDICACIÓN DEL ESTUDIANTE

Tipo	Horas	Porcentaje
Horas aprendizaje autónomo	90,0	60.00
Horas grupo pequeño	30,0	20.00
Horas grupo grande	30,0	20.00

Dedicación total: 150 h

CONTENIDOS

Introducción

Descripción:

Motivación. Algunos criptosistemas históricos: César, Vigenère, cifrado de un solo uso, Hill (mediante álgebra lineal modular). Principio de Kerckhoff.

Dedicación: 13h

Grupo grande/Teoría: 2h

Grupo pequeño/Laboratorio: 3h

Aprendizaje autónomo: 8h

Criptografía de clave pública

Descripción:

La idea de la criptografía de clave pública. El problema del logaritmo discreto. El intercambio de claves de Diffie-Hellman. El sistema criptográfico de clave pública de ElGamal. Ataques: algoritmo de Shanks (baby steps, giant steps), cálculo de índices.

Dedicación: 23h

Grupo grande/Teoría: 4h

Grupo pequeño/Laboratorio: 5h

Aprendizaje autónomo: 14h

RSA, pruebas de primalidad y factorización

Descripción:

El sistema criptográfico RSA. Cifrado y firma digital. Pseudoprimos, números de Carmichael. Pruebas de primalidad. Problemas de seguridad de RSA. Métodos de factorización: diferencia de cuadrados, método rho de Pollard, criba cuadrática.

Dedicación: 33h

Grupo grande/Teoría: 6h

Grupo pequeño/Laboratorio: 7h

Aprendizaje autónomo: 20h

Criptografía con curvas elípticas

Descripción:

Introducción a las curvas elípticas: ecuaciones de Weierstrass, ley de grupo, invariante j , puntos de torsión.

Curvas elípticas sobre cuerpos finitos y endomorfismo de Frobenius.

Criptosistemas basados en curvas elípticas: problema del logaritmo discreto, intercambio de claves (ECDH), cifrado de clave pública (El Gamal, ECIES), firmas digitales.

Factorización y pruebas de primalidad mediante curvas elípticas.

Dedicación: 73h

Grupo grande/Teoría: 14h

Grupo pequeño/Laboratorio: 15h

Aprendizaje autónomo: 44h

Criptografía basada en retículos

Descripción:

(Según el tiempo disponible) Retículos. Vectores cortos en retículos. Sistemas criptográficos basados en problemas difíciles de retículos. Algoritmo LLL. Criptografía postcuántica.

Dedicación: 8h

Grupo grande/Teoría: 4h

Aprendizaje autónomo: 4h

SISTEMA DE CALIFICACIÓN

Cualquier acto de fraude académico, plagio o uso o mera tenencia al alcance de medios no autorizados en cualquier actividad de evaluación comportará la calificación de cero (0) en la prueba o entrega afectada. Además, de acuerdo con la normativa de la Universidad, la posible derivación de los hechos para la apertura de un expediente disciplinario implicará que la asignatura quede en el estado provisional de "pendiente de evaluación" hasta la resolución del expediente. La gestión de estas incidencias se lleva a cabo de acuerdo con el [Marco de actuación para la integridad académica en la evaluación de la UPC](#).

Durante el semestre se realizarán dos exámenes de laboratorio (L1 y L2).

Al final del semestre, se entregará un informe final sobre un tema acordado con los profesores (FR) y se hará una presentación oral sobre ello (OP).

La calificación final se calculará mediante la fórmula $0,1 \cdot L1 + 0,1 \cdot L2 + 0,4 \cdot FR + 0,4 \cdot OP$.

BIBLIOGRAFÍA

Básica:

- Hoffstein, Jeffrey; Pipher, Jill; Silverman, Joseph H. An introduction to mathematical cryptography [en línea]. New York: Springer, 2014. Disponible a: <https://link-springer-com.recursos.biblioteca.upc.edu/book/10.1007/978-0-387-77993-5>. ISBN 9781493917105.

- Koblitz, Neal. A Course in number theory and cryptography. 2nd ed. New York: Springer-Verlag, cop. 1994. ISBN 0387942939.

- Washington, Lawrence C. Elliptic curves : number theory and cryptography [en línea]. Boca Raton [etc.]: CRC Press, 2008 [Consulta: 16/07/2026]. Disponible a: <https://www-taylorfrancis-com.recursos.biblioteca.upc.edu/books/mono/10.1201/9781420071474/elliptic-curves-lawrence-washington>. ISBN 9781420071467.

Complementaria:

- Delfs, Hans; Knebl, Helmut. Introduction to cryptography : principles and applications [en línea]. Berlin: Springer, 2015. Disponible a: <https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?pq-origsite=primo&docID=6314866>. ISBN 9783662479735.

- Katz, Jonathan; Lindell, Yehuda. Introduction to modern cryptography [en línea]. Boca Raton: Taylor & Francis Group, 2021.



[Consulta: 19/06/2025]. Disponible a :
<https://www.taylorfrancis-com.recursos.biblioteca.upc.edu/books/mono/10.1201/9781351133036/introduction-modern-cryptography-yehuda-lindell-jonathan-katz>. ISBN 9781466570269.
- Galbraith, Steven D. Mathematics of public key cryptography [en línea]. Cambridge University Press, 2012 [Consulta: 13/07/2022].
Disponible a :
<https://www.cambridge.org/core/books/mathematics-of-public-key-cryptography/DDDFA3874A53C4E6846EB3AB06161E43>. ISBN 9781107013926.